Linux Network Servers

Postfix

Na década de 70, as primeiras mensagens eram enviadas pela Arpanet, antecessora da atual Internet. A troca de mensagens era feita em sua maioria por estudantes, pesquisadores e profissionais dos grandes centros de pesquisa, restrita a poucos usuários que tinham acesso a essa rede. As mensagens eram enviadas através de um protocolo semelhante ao atual SMTP, que foi definido apenas em 1982.

O Sendmail era o servidor de correios mais utilizado na década de 90, causando amor e ódio aos administradores de sistema. Causava amor aqueles que tinham tempo de ler, estudar e compreender o seu funcionamento complexo e cheio de macros. Ódio para aqueles que precisavam apenas rotear suas mensagens e não havia necessidade de perder horas e mais horas tentando compreender seu funcionamento.

A sua forma monolítica também era um grande ponto negativo. Sendo apenas um único processo controlando todas as etapas de transmissão de email, o Sendmail apresentava inúmeras falhas de segurança, de maior risco quando executado em modo root. Muitos servidores eram invadidos por crackers e naturalmente os administradores de sistema procuravam alternativas. Na época não existiam muitas alternativas, os administradores continuavam a utilizar o Sendmail.

Em 1998 as primeiras versões do Postfix começaram a surgir. Wietse Venema é seu criador e possui inúmeros trabalhos relacionados à segurança da informação. Wietse é pesquisador da IBM até hoje. A primeira versão oficial do Postfix, em software livre, foi lançada em Dezembro de 1998.

Características do Postfix:

Sistema multitarefa - O Posftifx possui um conjunto de módulos que desempenham um papel específico para cada etapa do tráfego de e-mails, este comportamento permite melhor desempenho em equipamentos multiprocessados.

Separação de privilégios - O Postfix é executado em chroot que restringe o acesso a arquivos internos a jaula, separando assim muito de seus módulos.

Modular - É possível criar módulos para trabalhar em conjunto com o Postfix, tornando-o facilmente extendível.

Compatibilidade - O Postfix foi desenvolvido para suportar os formatos de armazenamentos de mensagens existentes.

Linux Network Servers

Os arquivos de configuração do Postfix, podem ser encontrados no diretório **/etc/postfix**, onde os seus principais arquivos são:

main.cf - Arquivo principal do Postfix onde ficam todas as configurações principais relacionadas ao funcionamento do Postfix.

master.cf - É o arquivo que controla a ação de cada daemon do Postfix, com ele podemos dizer quantos processos smtpd estarão em execução. Caso tenhamos uma estrutura grande de máquina, uma ajuste nesses daemons serão bem compensadoras em termos de performance.

MTA é o servidor de e-mails propriamente dito. Significa Mail Transport Agent. Exemplos de MTA: Postfix, Qmail, Exim, Sendmail etc.

MUA é um nome que é usado para designar os clientes de e-mail como, por exemplo, o Evolution, Kmail, Thunderbird, Outlook etc.

MDA é um intermediário entre o MTA e o MUA. Seu uso não é obrigatório, mas é útil para aplicar filtros antispam, remover vírus anexados nas mensagens e fazer encaminhamento de e-mails. Exemplos: Fetchmail e procmail.



Linux Network Servers

Vamos instalar o Postfix via aptitude:
aptitude install postfix

```
Os pacotes a seguir estão QUEBRADOS:
  exim4 exim4-config
Os NOVOS pacotes a seguir serão instalados:
  openssl-blacklist{a} postfix ssl-cert{a}
Os pacotes a seguir serão REMOVIDOS:
  exim4-daemon-light{a}
0 pacotes atualizados, 3 novos instalados, 1 a serem removidos e 13 não atualiza
dos.
É preciso obter 7575kB de arquivos. Depois do desempacotamento, 14,5MB serão usa
dos.
Os pacotes a seguir possuem dependências não satisfeitas:
  exim4-config: Conflita: postfix mas 2.5.5-1.1 será instalado.
  exim4: Depende: exim4-daemon-light mas não é instalável. ou
                  exim4-daemon-heavy mas não é instalável. ou
                  exim4-daemon-custom o qual é um pacote virtual.
As seguintes ações resolverão estas dependências:

Remover os pacotes a seguir:
exim4
exim4-base
exim4-config

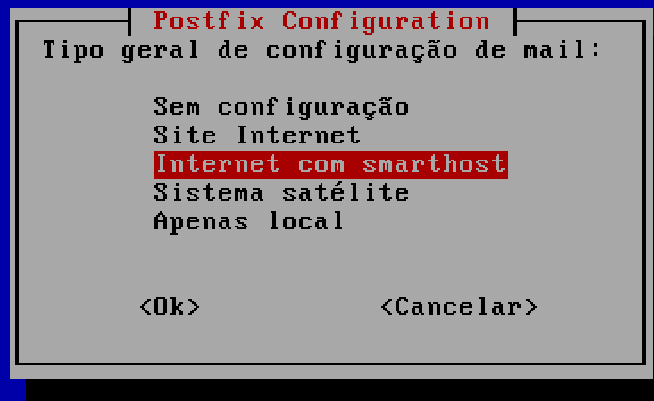
Pontuação é 251

Aceitar esta solução? [Y/n/q/?] _
```

Obs: No caso do Debian, quando instalarmos o Postfix, ele automaticamente remove o servidor padrão que é o Exim4.

Durante a instalação do pacote postfix uma janela será aberta a fim de coletar dados para gerar uma configuração padrão para o arquivo main.cf.

Linux Network Servers



A primeira pergunta se refere a função do servidor. A opção mais usada é "Internet Site".

Internet Site = Envia e recebe e-mails diretamente.

with smarthost = O servidor recebe mensagens, mas o envio fica a cargo de outro servidor.

Satellite system = O servidor envia mensagens através de outro servidor e não recebe mensagens.

Local only = Permite apenas que os usuários autenticados no servidor troquem e-mail entre si (usada em redes de terminais leve).

Linux Network Servers

Pode surgir uma pergunta sobre o domínio do servidor que será incluído nas mensagens enviadas. Se você está usando um servidor dedicado use o seu domínio registrado, por exemplo "4linux.com.br". Se for só para testes, deixe o padrão (não precisa alterar).

Pode surgir uma pergunta sobre Destinos aceitos pelo servidor. Este campo deve conter o nome da máquina (hostname), o domínio registrado (se houver), seguido de "localhost.localdomain" e "localhost", todos separados por vírgula e espaço.

Por exemplo:
m5, 4linux.com.br, localhost.localdomain, localhost

Qualquer e-mail que seja encaminhado para qualquer um dos endereços acima será colocado na caixa postal da conta do administrador.
Vejamos o arquivo de configuração main.cf:

vi /etc/postfix/main.cf

Banner que será mostrado nas conexões. É importante mudar.
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)

biff = no

Modificar o domínio caso o MUA's não fizer corretamente, mas deixamos ativado,
pois isso é trabalho do próprio MUA.
appending .domain is the MUA's job.
append_dot_mydomain = no

Tempo de aviso de mensagens de erro.
Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

Parâmetros de criptografia.
TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache

See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
information on enabling SSL in the smtp client.

Linux Network Servers

Nessa opção, precisamos colocar o hostname da máquina e o domínio que é
conhecido como FQDN.
myhostname = mail.4linux.com.br

Arquivos onde são configurados os alias de e-mails.
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases

Define a origem local, que por padrão é o mesmo FQDN que está em /etc/mailname.
myorigin = /etc/mailname

Domínios que o seu servidor pode receber mensagens.
mydestination = mail.4linux.com.br, localhost.4linux.com.br, , localhost

Essa opção só é usada se o seu servidor faz Relay para outros servidores
de e-mail.
relayhost =

Nesse campo deveremos colocar apenas os IP's que podem realmente fazer relay
em seu servidor.
CUIDADO, se adicionarmos IP's ou classes demais, o servidor poderá virar alvo
de spammers.
mynetworks = 127.0.0.0/8 192.168.200.0/24

Padrão de entrega das mensagens. Nesse caso é usado o mbox.
mailbox_command = procmail -a "$EXTENSION"

Tamanho máximo de caixa-postal para entrega local
mailbox_size_limit = 0

Em alguns clientes, podemos adicionar um sinal espcial ao endereço de e-mail
para direcionar mensagens a uma determinada pasta, por exemplo.
recipient_delimiter = +

Interfaces de rede a qual o Postfix pode fazer bind, ou seja, estabelecer
conexões. O padrão do Debian seria todas as interfaces.
inet_interfaces = all

Obs: O Postfix possui 525 linhas de configuração, só que somente as que estão setadas com valores diferentes do padrão é que são inseridas no arquivo.

Linux Network Servers

Visualize o formato do arquivo master.cf:
cat /etc/postfix/master.cf

Podemos agora reiniciar o postfix:
/etc/init.d/postfix restart

Veja se a porta 25 SMTP está pronta para receber conexões:
netstat -nlpt
fuser -v 25/tcp

Precisamos instalar um servidor POP3 para recebermos as mensagens. Nesse caso, usaremos o Qpopper:
aptitude install qppopper

O programa qppopper roda através do serviço inetd. Visualize o seu registro no arquivo inetd.conf:

cat /etc/inetd.conf

O serviço POP3 roda na porta 110, verifique se a conexãoe está ativa:

netstat -nlpt

fuser -v 110/tcp

Testando o Postfix

Por padrão, vamos utilizar o formato de armazenagem de mensagens mbox. Esse formato grava em um arquivo só todos as mensagens do usuário. Portanto os e-mails dos usuarios estão no /var/spool/mail e cada usuário terá um arquivo com o seu nome. Os usuários que estão criados no sistema GNU/Linux, são válidos como usuários do Postfix. Outro padrão que pode ser utilizado é o maildir que cria uma estrutura de diretórios para o usuário, onde cada mensagem é um arquivo separado.

Linux Network Servers

Vamos fazer o um teste e enviar uma mensagem via telnet:

telnet localhost 25

Comandos:

```
HELO - Inicia a conversa (identificação do emissor)
MAIL - Para indicar o emissor
RCPT - Para indicar o receptor
DATA - Texto do e-mail
.  - Indica o fim da mensagem
QUIT - fecha o telnet
```

Após o envio do e-mail, verifique se o usuário local recebeu a mensagem:

```
# cd /var/spool/mail
# ls
# cat usuario
```

Podemos receber a mensagem também por telnet acessando a porta 110:
telnet localhost 110

Obs: Por padrão o protocolo POP3 não é criptografado. Isso pode fazer com que um invasor capture os pacotes e consiga descobrir usuário e senha de quem está acessando. Caso seja necessário, podemos visualizar a fila de e-mails com o seguinte comando:
mailq

Linux Network Servers

Criando Alias no Postfix

Podemos criar alias para que um usuário possa receber vários e-mail's diferentes na mesma conta.

Edite o arquivo de alias e crie um para o seu usuário:
vi /etc/aliases
usuario_de_alias: usuario_existente

Para validar essas modificações e gerar o arquivo de hash, precisamos usar o comando postalias:
postalias /etc/aliases

Verifique se o arquivo aliases.db foi atualizado:
stat /etc/aliases.db

Agora podemos fazer um teste via telnet, enviando o e-mail para o usuário de alias:
telnet localhost 25

Se tudo deu certo, a mensagem destinada ao usuário de alias, vai ser armazenada na caixa postal do usuário real:
cd /var/spool/mail
cat usuario

Linux Network Servers

Courier Pop3 e Imap

Um servidor de e-mail não estaria completo sem a instalação de um "daemon" pop3 e imap. Para isso, iremos utilizar o software Courier e realizar a integração com o pam:

Para que o Courier funcione, é necessário instalar os seguintes pacotes:

```
# aptitude install Courier-authdaemon Courier-authlib courier-base
 courier-imap courier-pop
```

Após este passo, edite o arquivo de configuração do Postfix, acrescentando esta entrada:

```
# vim /etc/Postfix/main.cf
 home_mailbox = Maildir/
 mailbox_command = /usr/bin/procmail -a "$EXTENSION" DEFAULT=$HOME/Maildir/
MAILDIR=$HOME/Maildir/
```

Agora, ajuste o PAM para que nossos usuários possam efetuar autenticação:

```
# vim /etc/pam.d/pop3
        @include common-auth
        @include common-account
        @include common-password
        @include common-session

# vim /etc/pam.d/imap
        @include common-auth
        @include common-account
        @include common-password
        @include common-session

# vim /etc/pam.d/smtp
        @include common-auth
        @include common-account
        @include common-password
        @include common-session
```

Criando as caixas postais:

```
# maildirmake /home/aluno/Maildir
# maildirmake /home/aluno/Maildir/.Enviadas
# maildirmake /home/aluno/Maildir/.Rascunho
# maildirmake /home/aluno/Maildir/.Lixeira
# maildirmake /home/aluno/Maildir/.Spam
```

Linux Network Servers

O comando maildirmake é um comando do pacote courier.

Para maiores informações:
http://www.courier-mta.org/maildirmake.html

Ajuste as permissões do diretório aluno, para que ele possa receber as mensagens:
chown aluno:aluno -R /home/aluno

Assim como fizemos no teste do SMTP, utilizaremos o telnet para testar as portas IMAP e POP3.
telnet localhost 110
 user aluno
 pass 123456
 quit

Teste a porta 143, responsável pelo serviço IMAP:
telnet localhost 143
a login aluno 123456
logout

Se você conseguiu ler as mensagens, significa que o seu servidor está pronto para receber e transmitir mensagens através da internet.

Observação: Não esqueça de publicar o registro MX no seu DNS, configurar corretamente o campo TXT, também no DNS e configurar corretamente as consultas a DNS Reverso.